REMARKS – General

Claim Rejections under 35 USC §103(a):

The Office Action (OA) rejects claims 1-21 and 23-35 under 35 USC §103(a) as being unpatentable over Walker, US Published Patent Application No. 2004/0184614, in view of Kwon, US Published Patent Application No. 2006/0239334. Applicant respectfully traverses the rejection.

Comment on Applicant's Argument:

Applicant has argued, both in its response filed October 21, 2008 and July 3, 2009, and again here today, that the combination of Walker and Kwon fails to teach *the extraction* of a key from a scrambled signal. Applicant argues that instead, the combination of Walker and Kwon teaches the storage of keys *in a look-up table in the electronic device*. Messages received by the combination of Walker and Kwon include a *key indicator*. Applicant respectfully submits that a key indicator is not a unique key as recited in Applicant's independent claims. Further, the key indicator is not extracted from the message. Additionally, the key indicator is never examined. Finally, the key indicator of the references is never used to determine whether the message *was intended for the receiving device*. It is instead used to determine which decryption key will be used to unscramble the message – regardless of what device it was intended.

Applicant very respectfully submits that the Examiner has still failed to address this argument, which Applicant again submits here, with additional discussion in light of the "Response to Arguments" section of the most recent Office Action.

Relevant Recitation of Applicant's Claim 1:

Applicant's claim 1 recites in relevant part the following (with emphasis added by Applicant):

- **extracting** a unique identifier **from [a received] scrambled signal**; and

- **examining** the unique identifier that was **extracted from the scrambled signal** to **determine** if the signal **is intended for the communication device**.

Thus, as expressly recited in Applicant's claim 1, a scrambled signal is received. A unique identifier is then *extracted from that signal*. Once extracted, the unique identifier that was received in the scrambled signal is examined to determine if the signal is intended for the device. Applicant respectfully reminds the Examiner, "All the words in a claim must be considered in judging the patentability of that claim against the prior art." MPEP §2143.03, citing *In re Wilson*, 424 F.2d 1382, 1385 (CCPA 1970).

The Examiner's Rejection from the Combination as it Relates to These Steps:

In making the rejection, the Examiner submits that Walker teaches extracting a unique identifier from the scrambled signal at paragraph [0023]. See, e.g., Final Office Action, page 5. Specifically, the Examiner states, "…Walker teaches a method…extracting (read as isolate) a unique identifier from the scrambled signal (read as unique key used to communicate private secure messages, Pg. 3, [0023] and FIG. 4, item 54)…"

There is no other reference to "extracting" in the Office Action. Thus, in responding, Applicant turns its comments to the teachings of Walker for this step as it relates to the combination of Walker and Kwon. However, Applicant respectfully wishes to make clear that Applicant is not arguing against references individually. Applicant is arguing against the combination. However, to determine the scope and content of the combination of prior art references, as required by the Supreme Court in *Graham v. John Deere Co.*, 383 U.S. 1 (1966), which was reaffirmed by the Court of Appeals for the Federal Circuit in *KSR International Co. v. Tele-flex Inc.* (KSR), 550 U.S. 398 (2007), it is necessary to first understand what each reference teaches individually. Said differently, to know the sum of A and B, one must first define A and define B.

The Teaching of Walker:

For reference, Walker's paragraph [0023] is set forth here:

> [0023] Returning to FIG. 3, the method 100 stores specific group keys in the digital radio receiver in step 110. In step 112, method 100 receives and processes the data message. The data message is a data stream that is shown in FIG. 4, according to one example. The data message includes a data message header 50 and encrypted data 60 which includes a message 62. The data message header 50 includes non-encrypted data with key selectors 52A-52M that select which group keys are to be employed to decrypt the encrypted data 60. The data message header 50 may also contain message length message identification, and other unencrypted information that may be required to define the message. Each of the key selectors 52A-52M may include a binary bit of "0" or "1," with a binary bit "1" indicating use of the corresponding group key, and a binary bit "0" representing non-use of the corresponding binary key. Additionally, the data message header 50 includes a unique key indicator which indicates use of the key unique 74 stored in the digital radio receiver lookup table to communicate private secure messages. The encrypted data 60 includes an encrypted message 62 which, with the use of the appropriate decryption key(s), may be decrypted and presented to the vehicle and/or passengers. Additionally, the encrypted data includes a verification message 64 which verifies whether proper decryption of the data has been performed.

Applicant respectfully submits that there is no teaching whatsoever of extraction of a unique identifier in this paragraph. To the contrary, in the first sentence Walker describes "group specific [decryption] keys" being *stored* "in the digital receiver in step 110," which occurs ***before any signal is received.*** Note that the received signal does not occur until step 112, while the storing step occurs at step 110.

Next, in this paragraph Walker states, "The data message header 50 includes non-encrypted data with key selectors 52A-52M that select which group keys are to be employed to decrypt the encrypted data 60." Applicant respectfully notes that there is no reference to a unique identification key whatsoever. Instead, there is reference only to "key selectors" which are used to select decryption keys that have *already been stored in the radio*. These decryption keys will be used to decrypt the message.

This is true because Walker expressly teaches how these key selectors are used. "Each of the key selectors 52A-52M may include a binary bit of "0" or "1," with a binary bit "1" indicating use of the corresponding group key, and a binary bit "0" representing non-use of the corresponding binary key." Thus, the key selector is indicative only of the *use* of a key that is *already stored* in the radio. Applicant further notes that these key selectors are not extracted from the message and examined to determine if the message is indeed intended for the electronic device – they are instead only read to determine which of the pre-stored keys in the radio are to be used. Walker makes this clear by stating, "Additionally, the data message header 50 includes a unique key indicator ***which indicates use of the key unique 74 stored in the digital radio receiver lookup table*** to communicate private secure messages." Emphasis added. The remainder of paragraph [0023] describes how the message is decrypted.

Applicant respectfully submits that there is absolutely no extraction and examination to determine if the message is intended for the device occurring here whatsoever. Applicant respectfully submits that there is no such extraction and examination taught in the remainder of Walker either. The keys are always "…stored in the digital radio receiver lookup table to communicate private secure messages." *Id.* This storage occurs before any receipt of a message, as set forth in both FIG. 3 and paragraph [0023]. The messages only include key indicators indicating which decryption key to use.

To repeat, when a mobile communication device receives the message, it looks to the header to determine **which stored stored key to use**. Walker, par. [0024]. The encryption keys, which are based upon identifiers corresponding to the mobile device, are **not stored in the message**. Rather, they are stored in the mobile device. *Id.* Walker expressly teaches this at par. [0020] and par. [0023]: "[M]ethod 100 creates a unique decryption key based on the radio identification number and the vehicle identification number in step 106." Further, "[M]ethod 100 stores specific group keys in the digital radio receiver in step 110."

For these reasons, Applicant respectfully submits that there is no extraction and examination of a key from a scrambled message to determine whether the message is intended for the electronic device taught by Walker.

Combining Walker with Kwon:

Turning now to Kwon, the addition of Kwon to Walker fails to remedy this deficiency, as Kwon fails to teach any unique identifier being stored in the scrambled message either. *As no unique identifier is stored therein, none can be extracted. Nor can any be examined.*

To the contrary, Kwon teaches a long code mask being generated from an Electronic Serial Number corresponding to a mobile device. At paragraph [0016], Kwon states, "The output of the long code generator 232 is decimated into a PN (Pseudo-Noise) sequence by the decimator 234 using the long code mask 250 generated from an ESN (Electronic Serial Number) allocated by the respective secondary stations."

This long code mask is used to encrypt or decrypt the message. It is not a unique identifier stored within the message. To the contrary, it is stored in the receiver of Kwon. *See, e.g.,* Kwon par. [0050]. To be sure, the only "insertion" of information into the message taught by Kwon is the "Power Control Bit" into the "PCB position" for "…controlling the transmission power from the secondary station." Kwon, par. [0017]. Kwon inserts this bit so that the message can hop according to a hopping pattern negotiated between the transmitter and receiver. Kwon, Abstract.

Despite suggestions to the contrary by the OA, there is no insertion of a unique identifier into the scrambled message in the teachings of Kwon. **Consequently, there can be no extraction or examination.** Kwon only teaches a long code mask that, in conjunction with a decimator, creates a long code. *See, e.g.,* Kwon paragraphs [0050] and [0051].

When Kwon is combined with Walker, a scrambled message is decoded – as determined by the one bit key selector of Walker – by either the encryption key of Walker that is stored in the memory of the mobile device of Walker, or by the long code mask of Kwon that is stored in the receiver of Kwon. (The OA relies on the encryption key of Walker, for instance, in the rejection to claim 1, while relying on the long code mask of Kwon in the rejection to claim 15.) Applicant respectfully submits there is simply no teaching in the combination of Walker and Kwon of a unique identifier being extracted from the encrypted message and examined to determine if the message is intended for the device.

By contrast, Applicant claims a method and system where a unique identifier is **extracted from** the scrambled signal. This unique identifier, when the scrambled signal is received (e.g., claims 1 and 8), is examined to determine if the signal is intended for the communication device. The unique identifier, where inserted (e.g., claim 15), is to ensure that the scrambled message is directed to the proper mobile device. The unique identifier can be inserted into, for example, the power control sections of the scrambled message (claim 17). As such, Applicant respectfully submits that independent claims 1, 8, 15, 23, 28, and 32 are therefore allowable over the combination of Walker and Kwon.

Advantages of Applicant's Invention over the Combination of Kwon and Walker:

The combination of Walker and Kwon leaves open the possibility of decryption errors. For example, a message received by the combination of Walker and Kwon must be decrypted by either the encryption key of Walker or the long code mask of Kwon. As noted by Applicant, "…decoding errors can lead to cyclic redundancy code checking failures, the mobile station cannot distinguish between an erasure or improperly received signal due to decoding error and a frame intended for another mobile station that uses the same forward dedicated control channel." Applicant's specification, paragraph [0005]. By contrast, as recited in Applicant's claim 8, where the cyclic redundancy coded signal fails the cyclic redundancy code check in Applicant's invention, the system can still examine the unique identifier of the scrambled signal to determine if the signal is intended for the mobile communication device because it is inserted into portions the scrambled signal. The combination of Kwon and Walker simply cannot reconcile decoding errors in this fashion, as any uniqueness is found only in the decryption keys, not in the messages themselves.

Applicant's Response to Explanation Set Forth in the Rejection:

As noted above, the Examiner states that Walker does teach extracting. The Examiner states at page 5 of the most recent Office Action that Walker teaches "extracting" as follows: "…extracting (read as isolate) a unique identifier from the scrambled signal (read as unique key used to communicate private secure messages, Pg. 3, [0023] and FIG. 4, item 54)…"

Applicant respectfully disagrees. Walker never mentions the word "isolate" or any variation thereof in its specification. It most certainly never mentions it at paragraph [0023], in FIG. 4, or in relation to item 54.

There is no teaching of a key being included in the message of Walker. The fact that the words "unique key" appear in FIG. 3 is in no way indicative of key inclusion or a corresponding extraction thereof occurring. As explained above, Walker expressly states that all keys are stored in the mobile device. It is clear from the description of FIG. 3 set forth by Walker that the "unique key" appearing in FIG. 3 is short for "unique key indicator" as there is no description of a key being included or embedded in Walker's message whatsoever. The only reference to anything "unique" occurring in paragraph [0023] is with respect to unique key **indicators**. Applicant respectfully reminds the Examiner, "A decision to make or maintain a rejection in the face of all the evidence must show that it was based on a totality of the evidence." *In re Eli Lilly & Co.,* 902 F.2d 943 (Fed. Cir. 1990). When the totality of Walker and Kwon are considered, to be sure, it is clear that keys are not stored in any messages. They are instead stored within the device.

Applicant's Response to Main Explanation Set Forth in "Response to Arguments" Section in Most Recent Office Action:

Applicant initially notes the Examiner *acknowledges* Applicant's point of there never being an extraction of a unique key from a scrambled message in Walker. To the contrary, the Examiner acknowledges that the keys are stored in the electronic device. Specifcally, at page 2 of the most recent Office Action, the Examiner states:

> The *receiver* [of Walker] further *includes* a data decryption circuit including memory *for storing one or more groups of decryption keys* based on a characteristic of the receiver environment. The data decryption circuit selects a group decryption key *base on the key selector* and decrypts the message based on the selected group decription key.

Applicant respectfully asks, where is there a teaching of an extraction of a key in this passage? Key indicators are not keys. As expressly acknowledged by the Examiner, all keys are stored in the device. By contrast, Applicant's invention as recited in claim 1 teaches extracting the key from a scrambled message.

Further, Applicant's invention does not use the extracted key for decryption, but rather for determining "…if the signal is intended for the communication device." Applicant respectfully asks, where is there a teaching of such a determination in either Walker or Kwon? It is certainly not set forth in the Examiner's Response to Arguments. Applicant respectfully reminds the Examiner that "…the analysis supporting a rejection under 35 USC §103 should be made explicit…rejections on obviousness cannot be sustained with mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support a legal conclusion of obviousness." MPEP §2142, citing *KSR International Co. v. Tele-flex Inc.* (KSR), 550 U.S. 398, 412 (2007), citing *In re Kahn*, 441 F. 3d 977, 988 (CA Fed. 2006).

Applicant's Response to Remainder of "Response to Arguments" Section:

The Examiner states, "Walker discusses a packetized data stream format that includes a header section with key selectors, group keys…" Applicant respectfully disagrees. Applicant has shown above that no keys are included in the messages of Walker. There are only key indicators. All keys, as acknowledged by the Examiner, are stored in the electronic device.

The Examiner states, "…a unique key is extracted (isolated and applied separately to indicate a private message) from the encrypted data." Applicant respectfully disagrees. As set forth in Walker's paragraph [0023], there are only key indicators in the message. The key indicator is read and "…indicates use of the unique key 74 ***stored in the digital radio receiver lookup table***…" In Applicant's invention, by contrast, an actual key – not a key indicator – is stored within the message. Applicant respectfully reminds the Examiner, "All the words in a claim must be considered in judging the patentability of that claim against the prior art." MPEP §2143.03, citing *In re Wilson*, 424 F.2d 1382, 1385 (CCPA 1970).

The Examiner states, "The format includes a unique key indicator that indicates a private secure message for a specific device." Applicant respectfully disagrees. As noted in the preceding paragraph, the key indicator does not indicate a private message. It instead "…indicates use of the unique key 74 ***stored in the digital radio receiver lookup table***…" The key in the look up table "…allows for *private decryption* to communicate secure data to a single receiver." Walker, paragraph [0020]. The key indicator has no bearing on the type of message being transmitted.

The Examiner states, "Walker clearly reads on the argued limitations of 'extracting a unique identifier from the scrambled signal.'" Applicant respectfully disagrees. As shown above, there is no extraction of a key from a message in Walker because there is no key in the message of Walker. As acknowledged by the Examiner, the keys are pre-stored in the electronic device.

The Examiner states, "Walker clearly reads on the argued limitations of…examining the unique identifier extracted from the scrambled signal…" Applicant respectfully disagrees. If no key is extracted, how can one be examined?

The Examiner states, "The applicant argues specifically that Walker and Kwon do not teach a unique key identifier." This is partially correct. Applicant argues that Walker and Kwon do not teach **extracting** a unique identifier from a scrambled message. Applicant readily admits that Walker teaches the inclusion of a decryption key identifier in its message. However, a decryption key indicator is **not** a unique identifier.

The Examiner states, "The Applicant argues that Walker fails to teach 'embedding a unique identifier into a scrambled message.' However, the Applicant has not used this claim language." Applicant respectfully submits that it is in no way arguing that embedding is recited, for example, in claim 1. Applicant argues the embedding step to make the point that if no unique identifier is embedded, none can be extracted because none is there.

The Examiner states, "The applicant argues that Kwon fails to teach 'any unique identifier being stored in a scrambled message.' Again, nowhere in the actual claim language is this found." In response, Applicant simply poses this question: How can an extraction of a unique identifier from a message be present in Kwon when no unique identifier is ever placed in Kwon? As with the preceding paragraph, Applicant argues the storing step to make the point that if no unique identifier is embedded, none can be extracted because none is there.

For the reasons set forth above, Applicant respectfully submits that independent claims 1, 8, 15, 23, 28, and 32 are therefore allowable over the combination of Walker and Kwon. Applicant respectfully requests reconsideration of the rejection to these claims, as well as the claims depending from these claims, in light of these comments.

CONCLUSION

For the above reasons, Applicant believes the specification and claims are now in proper form, and that the claims all define patentably over the prior art. Applicant believes this application is now in condition for allowance, for which it respectfully submits.

Respectfully submitted,

Philip H. Burrus, IV
Attorney for Applicants
Registration No.: 45,432
404-797-8111
404-880-9912 (fax)
pburrus@burrusiplaw.com